

Опис освітнього компонента вільного вибору	
Дисципліна	Вибірковий освітній компонент 3 «Програмування криптографічних алгоритмів та методів»
Рівень ВО	перший (бакалаврський) рівень
Назва спеціальності/освітньо-професійної програми	122 Комп'ютерні науки / Комп'ютерні науки та інформаційні технології
Форма навчання	Денна
Курс, семестр, протяжність	4 (8 семестр), 4 кредитів ЄКТС
Семестровий контроль	Залік
Кількість кредитів / Обсяг годин (усього: з них лекції/практичні)	120 год, з них: лекції - 20 год, практичні - 20 год
Мова викладання	українська
Кафедра, яка забезпечує викладання	комп'ютерних наук та кібербезпеки
Автор дисципліни	Кандидат фізико-математичних наук; доцент кафедри комп'ютерних наук та кібербезпеки Глинчук Людмила Ярославівна
Короткий опис	
Вимоги до початку вивчення	Теорія ймовірностей, Алгебра, Програмування
Що буде вивчатися	Основні симетричні та асиметричні криптографічні алгоритми та методи, хеш-функції, електронний цифровий підпис, криптопротоколи та ін. Область їх застосування, особливості та суть. Особливості програмування криптографічних алгоритмів та вибір мови програмування для завдань захисту.
Чому це цікаво/треба вивчати	Криптографічні алгоритми мають певну складність та цікаві за своїм змістом та використанням. Дисципліна дасть можливість не тільки зрозуміти криптографічний захист, а і здобути навички програмування таких методів.
Чому можна навчитися (результати навчання)	ПРН16. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних
Як можна користуватися набутими знаннями й уміннями (компетентності)	ЗК2. Здатність застосовувати знання у практичних ситуаціях. ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності. ЗК6. Здатність вчитися й оволодівати сучасними знаннями. ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.
Інформаційне забезпечення та/або web-покликання	